

日 本 国 特 許 庁
JAPAN PATENT OFFICE

(4)
Jc971 U.S. PRO
10/083758
02/26/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2001年 9月28日

出 願 番 号
Application Number:

特願2001-302469

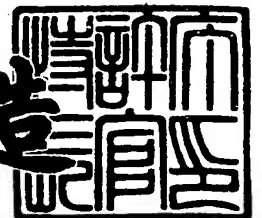
出 願 人
Applicant(s):

富士通株式会社

2001年12月 7日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3106976

【書類名】 特許願

【整理番号】 0150992

【提出日】 平成13年 9月28日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16
H04L 12/46
H04L 12/00

【発明の名称】 通信装置

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 北村 卓也

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100090011

【弁理士】

【氏名又は名称】 茂泉 修司

【手数料の表示】

【予納台帳番号】 023858

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704680

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信装置

【特許請求の範囲】

【請求項1】

ユーザ端末とネットワーク接続業者機器との間の通信を行う接続処理部と、
送信元のユーザ端末から送信されたデータに含まれるデータリンク層情報を読み出し、該データリンク層情報にネットワーク接続業者機器への通信要求情報又は宛先ユーザ端末とのショートカット通信の要求情報が含まれているか否かを監視する情報監視部と、

該データリンク層情報が該通信要求情報を含む場合には該ネットワーク接続業者機器に該データを出力し、該データリンク層情報が該ショートカット通信の要求情報を含む場合には該宛先ユーザ端末に該データを出力する制御部と、

を備えることを特徴とした通信装置。

【請求項2】 請求項1において、

該ショートカット通信の要求情報は、該データリンク層情報にカプセル化されていることを特徴とする通信装置。

【請求項3】 請求項2において、

該ショートカット通信の要求情報は、該データリンク層情報中のイーサネットのプロトコルにカプセル化されていることを特徴とする通信装置。

【請求項4】 請求項2において、

該通信要求情報はPPPoEのプロトコルであり、該ショートカット通信の要求情報は、該データリンク層情報中の該PPPoEのプロトコルにカプセル化されていることを特徴とする通信装置。

【請求項5】 請求項1から4のいずれかにおいて、

該データリンク層情報は認証情報を含み、該制御部は、該認証情報に基づいて該送信元ユーザ端末と該宛先ユーザ端末とのショートカット通信を許容するか否かを判定し、該ショートカット通信を許容する場合に、該接続処理部に該宛先ユーザ端末へ該データを出力させることを特徴とする通信装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は通信装置に関し、特にユーザ端末とネットワーク接続業者機器との間の通信を行う通信装置に関するものである。

ISDNや電話回線を用いたダイヤルアップによって実現されていた従量制課金のインターネット／企業網アクセスシステムは、ADSL (Asymmetric Digital Subscriber Line: 非対称デジタル通信網) /FTTH (Fiber To The Home: 光ファイバ網) 等の新しい高速伝送技術の出現や、キャリア間の競争激化によって、専用線と同じ定額制課金でありながら安価であるシステムへと急速に移行しつつある。

【 0 0 0 2 】

一般家庭向けのサービスとしては、第一にネットワーク接続が容易であることが求められており、ユーザに提供されるインタフェースとしてはイーサネットが望ましい。一方、インターネット接続サービスを提供するISP(Internet Service Provider)としては、従来のダイヤルアップシステムと同じ仕組み(PPP: Point-to-Point Protocol)でユーザ管理を行いたいという要求がある。

【 0 0 0 3 】

この2つの要求を満たすために考え出されたのが、PPPをイーサネット上にカプセル化するPPPoE (PPP over Ethernet) であり、IETF (Internet Engineering Task Force) のドキュメントRFC2516で規定されている。世界各国でこの技術を用いたサービスが注目されている。

【 0 0 0 4 】

【従来の技術】

ADSLやFTTHを適用したアクセス回線では、ユーザ側の装置はキャリアの装置以外にはアクセスすることができない仕組みとなっているが、今後、イーサネットを直接光ファイバに乗せて、電柱の上などでスイッチングを行うイーサネットアクセス網が整備されて行くことが予想される。

【 0 0 0 5 】

このようなイーサネットアクセス網は、後述する図1に示すような構成となっている。すなわち、ユーザ端末11, 12はONU13, 14及び通信装置15を介してISPの

端末であるエッジ装置18に接続される。このエッジ装置18を介してユーザ端末11, 12はインターネットINETへのアクセスを行う。

【0006】

ここではセキュリティ上の配慮から、IEEE802.1Qで定義されるVLAN(Virtual LAN)等の技術を用いて、ユーザ端末11, 12はエッジ装置18以外にはアクセスすることができないようにしている。

すなわち、本来イーサネットであれば、例えば隣の家のパソコンと直接通信することも可能であるが、悪意を持った第三者が存在し、フレームを盗み見たり、他人のIDを用いてネットワークへアクセスしたりすることが可能となってしまう。

【0007】

特にセキュリティに関する知識の無い初心者等は、これらに対して防御することが難しいため、セキュリティ対応がなされているエッジ装置18を介して通信する仕組みとしている。

上述のPPPoEを用いた仕組みによると、ユーザ端末11は、ユーザ端末12と通信をするために、フレーム23がONU13及び通信装置15を介して一旦エッジ装置18に流れ、そこで折り返されて通信を行うことになる。さらに、ユーザ端末11とユーザ端末12とがそれぞれ異なるISPに加入している場合には、インターネットを経由して通信を行うことになる。

【0008】

これは帯域の無駄になるだけでなく、エッジ装置18の負荷を増大させることになってしまうという問題がある。今後、オンラインゲームの普及や、地域に密着したアプリケーションの出現、様々な機器のネットワークサポートにより、物理的に距離の近い装置間での通信の比率が高まっていくことが予想される。

【0009】

【発明が解決しようとしている課題】

しかしながら、現状のシステムの延長では、ユーザ端末1台当たりの使用帯域が10倍になったとして、単純計算で現状の10×ユーザ数倍の処理を行う性能を持ったエッジ装置が必要となってしまう。

【0010】

そこで単純にイーサネットを用いたシステムを構築してしまうと、前述のセキュリティ上の問題が発生することから、現状のセキュリティレベルを維持したまま、ショートカット通信（エッジ装置18を介さずに行う通信）が可能となるような仕組みが必要である。

【0011】

すなわち、ユーザ端末同士でシステムを構築することなく、またエッジ装置18を介さないでショートカット通信を行うには、ユーザ端末11とユーザ端末12とを接続する通信装置15が、ユーザ端末11、12から受け取ったフレームをエッジ装置18に送信することなく直接に宛先となるユーザ端末に送信することが必要となる。

【0012】

従って本発明は、ユーザ端末とネットワーク接続業者機器との間の通信を行う通信装置において、ユーザ端末間でショートカット通信させることにより通信の高速化を図ることを目的とする。

【0013】

【課題を解決するための手段】

上記の目的を達成するため、本発明に係る通信装置は、ユーザ端末とネットワーク接続業者機器との間の通信を行う接続処理部と、送信元のユーザ端末から送信されたデータに含まれるデータリンク層情報を読み出し、該データリンク層情報にネットワーク接続業者機器への通信要求情報又は宛先ユーザ端末とのショートカット通信の要求情報が含まれているか否かを監視する情報監視部と、該データリンク層情報が該通信要求情報を含む場合には該ネットワーク接続業者機器に該データを出力し、該データリンク層情報が該ショートカット通信の要求情報を含む場合には該宛先ユーザ端末に該データを出力する制御部とを備えたことを特徴としている。

【0014】

すなわち本発明においては、送信元のユーザ端末から送信されたデータに含まれるデータリンク層情報を読み出し、該データリンク層情報がネットワーク接続

業者機器への通信要求情報を含む場合には該ネットワーク接続業者機器に該データ群を出力するという既存のプロトコルによる通信機能を維持しつつ、該データリンク層情報が宛先ユーザ端末とのショートカット通信の要求情報を含む場合には直接該宛先ユーザ端末に該データを出力することができる。

【 0 0 1 5 】

これにより、送信元のユーザ端末から宛先ユーザ端末に出力されるデータ量が膨大になった場合でも該ネットワーク接続業者機器を必要以上に拘束する必要がなくなり、以って通信の高速化も図ることができる。（請求項1／付記1）

また、ショートカット通信の要求情報は、データリンク層情報にカプセル化してもよい（請求項2／付記2）。

【 0 0 1 6 】

また、ショートカット通信の要求情報は、データリンク層情報中のイーサネットのプロトコルにカプセル化してもよい。

従って、イーサネットのデータリンク層情報を読み出すときに、該データリンク層情報に含まれる、例えばPPPoE等のプロトコル情報を読んでいるか否かに関係無く該ショートカット通信の要求情報が読み出されるため、PPPoE等のプロトコル情報等による接続状態の維持が必要無くなり、その結果、その接続状態のオーバーヘッドを無くすことができ、帯域の利用効率を上げることができる。（請求項3／付記3）

また、通信要求情報はPPPoEのプロトコルとし、ショートカット通信の要求情報は、該データリンク層情報中の該PPPoEのプロトコルにカプセル化してもよい。

【 0 0 1 7 】

従って、既存のユーザ端末と接続業者端末の間に用いられている例えばPPPoE等のプロトコルを有効利用した上で、ユーザ端末間のショートカット通信を図ることができる。（請求項4／付記4）

また、データリンク層情報は認証情報を含み、制御部は、認証情報に基づいて送信元ユーザ端末と宛先ユーザ端末とのショートカット通信を許容するか否かを判定し、該ショートカット通信を許容する場合に、該接続処理部に該宛先ユーザ

端末へ該データを出力させてもよい。

【 0 0 1 8 】

従って、ショートカット通信にあたって無条件に宛先端末にデータを送るのではなく、相手先との確認を必要とするようになるので、不正アクセスの防止を図ることができる。（請求項5／付記5）

また、認証情報はRADIUSのフォーマットに基づく形式で記述し、該制御部は該認証情報をRADIUSサーバに出力してその照合結果を参照することでショートカット通信を許容するか否かを判定してもよい。

【 0 0 1 9 】

従って、ショートカット通信にあたりRADIUSのフォーマットによる信頼性の高い認証が行われるため、ショートカット通信における不正アクセスの防止を図ることができる。（付記6）

また、制御部は、送信元ユーザ端末及び宛先ユーザ端末のアドレス情報を通信ポートに対応付けて保持するメモリを備え、該データが該ショートカット通信の要求情報を含む場合に、該ショートカット通信の要求情報に含まれるアドレス情報に対応した通信ポートを通して該接続処理部に該データを出力させてもよい。

【 0 0 2 0 】

従って、該直接通信の要求情報に含まれるアドレス情報を参照するだけでショートカット通信を行うことができる。（付記7）

また、情報監視部が通信要求情報を読み出した結果、ネットワーク接続業者機器との接続の中断要求情報が含まれている場合、接続処理部は該ネットワーク接続業者機器との通信を中断してもよい（付記8）。

【 0 0 2 1 】

また、制御部は、データリンク層情報に含まれるMACアドレスの書き換えにより該データの出力先を制御してもよい（付記9）。

また、制御部は、送信元ユーザ端末からのデータリンク層情報に含まれる認証情報と宛先ユーザ端末からの認証情報を照合することにより、該送信元ユーザ端末と該宛先ユーザ端末とのショートカット通信を許容するか否かを判定してもよい（付記10）。

【 0 0 2 2 】

また、情報監視部が該通信要求信号を読み出した結果、該ネットワーク接続業者機器との接続の再開要求情報が含まれている場合、該接続処理部は該ネットワーク接続業者機器との通信を再開してもよい（付記11）。

【 0 0 2 3 】

【発明の実施の形態】

図1は、本発明が適用されるネットワークの構成例を示した図であり、このネットワークは、ユーザ端末11、12、ONU（Optical Network Unit：光回線終端装置）13、14、通信装置15～17、エッジ装置18～20、RADIUSサーバ21、及びオンラインゲームサーバ22で構成されている。

【 0 0 2 4 】

ユーザ端末11、12は、それぞれONU13、14にイーサネットに接続されており、これらのONU13、14を経由して本発明の通信装置15に共通接続されている。ONU13、14は、光ファイバの加入者宅に設置することで、パーソナルコンピュータ（PC）などのユーザ端末を光ファイバに接続するための機器である。

【 0 0 2 5 】

なお、ネットワーク上には通信装置16、17も図示されているが、これらにも同様にそれぞれ複数のユーザ端末（図示せず）が接続されている。

通信装置15は、プロバイダの端末を構成するエッジ装置18に接続されている。通信装置15を介してユーザ端末11、12とエッジ装置18を接続することでインターネットへのアクセスを可能にしている。

【 0 0 2 6 】

エッジ装置18には、認証用のRADIUSサーバ21が接続されていると共に、キャリア網CNを通してエッジ装置19、20に接続されている。エッジ装置19、20はインターネットINETの各サービスプロバイダ（ISP）を構成しており、さらにインターネットINETを経由してオンラインゲームサーバ22が接続されている。

【 0 0 2 7 】

このような構成により、ユーザ端末11、12がネットワーク上でゲームを楽しむ場合、以上のネットワーク経路を経てオンラインゲームサーバ22に辿りつくよう

になっている。

図1の下部に示したフレーム23～27は、ユーザ端末11、12からオンラインゲームサーバ22まで送信されるデータのプロトコルを概略的に示したものであり、本発明に関連するデータリンク層とネットワーク層についてのみ示している。

【 0 0 2 8 】

まず、フレーム23については次の通りである。ユーザ端末11、12とONU13、14とは10BASE-T等のLAN用ケーブル（UTP：Unshielded Twisted Pair／無シールドツイストペアケーブルや光ファイバ）で接続され、イーサネットプロトコルにより通信が行われる。

【 0 0 2 9 】

このため、ユーザ端末11、12は、ネットワーク層のIPアドレス、データリンク層のPPP、PPPoE、及びイーサネットプロトコルを含む構成のフレーム23をONU13、14にそれぞれ送信する。

なお、例えばフレーム23に示すイーサネット（UTP）は、物理層がUTPや光ファイバであることを示しており、以下、最下層で括弧書きしたものは物理層の内容を示す。

【 0 0 3 0 】

フレーム24については、ONU13、14と通信装置15とが、フレーム23の場合と同様にイーサネットプロトコルにより通信しているため、フレーム23と同じフォーマットを有する。従って、ONU13、14はフレーム23のフォーマットのままフレーム24として通信装置15に送信する。従って、フレーム24の物理層はUTPから光ファイバに変わるが、データリンク層には影響が無い。

【 0 0 3 1 】

フレーム25については、通信装置15とエッジ装置18とが、フレーム24と同様に光ファイバのイーサネットプロトコルにより通信しており、物理層は変わらない。従って通信装置15は、フレーム25に示す如く、フレームを書き換えずにエッジ装置18に送信する。

【 0 0 3 2 】

フレーム26については、エッジ装置18とエッジ装置19及び20とは、ATM（Async

hronous Transfer Mode：非同期転送モード）を介して接続されるため、PPPoEではなくL2TP(Layer 2 Tunneling Protocol)により通信が行われるフォーマットになっている。

【 0 0 3 3 】

従ってエッジ装置18は、フレーム26に示す如く、データリンク層のPPPoEをL2TPに、そしてイーサネットプロトコルをIPアドレスとATMの形式にそれぞれ書き換えて、エッジ装置19又は20に送信する。

フレーム27については、エッジ装置19及び20がインターネットINETを通してオンラインサーバ22に接続されているので、インターネットINET上での接続はイーサネットによるものとは限らず、また接続媒体も特定されていない。

【 0 0 3 4 】

しかしながら、宛先となるIPアドレスに基づき送信経路が決定されるため、エッジ装置19又は20は、フレーム27に示す如く、フレーム26のIPアドレスはそのまま、残りをフレーム27が通る経路に合わせて書き換えてオンラインゲームサーバ22に送信することになる。

【 0 0 3 5 】

オンラインゲームサーバ22からユーザ端末11、12へのフレームは、上記の流れを逆に戻りながら書き換えられる形となる。

図2は、本発明に係る通信装置の構成例を示しており、制御部30、メモリ31、イーサネット処理部32、情報監視部33、及びRADIUS制御部34により構成されている。これらの各部は、CPU、ROM、RAM等を用いることができる。

【 0 0 3 6 】

この内、制御部30は、フレーム情報の変更やテーブルの管理を含む本発明に関する全体的な制御を行うものである。メモリ31は、制御部30の処理において必要なデータ等を保持する。イーサネット処理部32は、PPPoEの処理等の通信処理を行う。

【 0 0 3 7 】

情報監視部33は、受信したフレームの内容を識別するものであり、RADIUS制御部34は、RADIUSサーバ21とのフレームの送受信処理を行う。

実施例 (1) : 図3~13

図3及び図4は、図2に示した通信装置の動作実施例(1)のフローチャートを示したものであり、図5は通信装置15で保持される各接続端末に対応したテーブルを示し、図6~11は、ユーザ端末11と通信装置15との間でやり取りされるフレームのフォーマットを示している。以下、これらの図を用いて図1及び図2に示した通信装置15の動作実施例(1)を説明する。

【0038】

まず、図1のユーザ端末11, 12はそれぞれエッジ装置19, 20に接続されるために、IPアドレスの割当を受けているものとし、それぞれ独立してインターネットINETに接続されており、かつインターネットINETを経由してのみ通信が可能な状況にあるものとする。

【0039】

ここで、ユーザ端末11, 12を使用しているユーザAとユーザBは、あるWeb掲示板にて同じMA(Message Area)配下で同じアクセスサービスを利用していることを知り、2人はショートカットサービスを用いてオンラインゲームで対戦することにした。

【0040】

ここで話を簡単にするため、ショートカット通信中のフレーム23(24)の流れについては、ユーザ端末11からユーザ端末12へのみ流れるものとし、ショートカット通信の開始・中断・再開・終了についてはユーザ端末11及びユーザ端末12の両方からフレーム23(24)を受け取るものとする。ユーザ端末12からユーザ端末11へフレームを送信する場合についても同様である。なお、フレーム23と24とは同一内容である。

【0041】

まず制御部30は、通信開始のための初期動作を行う(ステップS1)。次にイーサネット処理部32はフレーム待ち状態となり、制御部30は、イーサネット処理部32がフレーム24を受信したか否かを判定する(ステップS2)。

フレーム24を受信していなければ、制御部30は、図4に示す如くカウントされるTTL(Time To Live)値が、“0”となっているポートの登録を図5に示すテ-

ブルTBLから削除する（ステップS3）。

【 0 0 4 2 】

TTL値は1秒毎に“1”ずつ値が減っていく。このTTL値が“0”になった情報についてはテーブルTBLからエントリの削除を行う。このTTL値は、何らかのフレームがユーザ端末11, 12から送信されて来る度に初期値にリセットされる。

具体的には、図4に示す通り、制御部30は、タイマが1秒経過するのを待つ（ステップS27）。1秒経過したら、制御部30は各ポートのTTL値が“0”であるか否かを判定する。“0”の場合はTTL値を変更する必要がないため、そのままステップS27に戻る（ステップS28）。なお、TTL値が“0”になったポートP1,P2に対応するデータは、前述の通りテーブルTBLから削除の対象となる。

【 0 0 4 3 】

TTL値が“0”でない場合は、制御部30は、各ポートのTTL値から“1”だけ減算し、ステップS27に戻る（ステップS29）。なお、このTTL値の処理は、制御部30により図3のフローチャートからは独立して実行される。

次に図5に示すテーブルTBLの内容について説明する。通信装置15はポートP1,P2（図1参照）を有し、ポートP1,P2を介してユーザ端末11, 12と通信するが、メモリ31ではポートP1,P2に対応させてMACアドレス、PPPoEセッションID、IPアドレス、グループID、キャリア網接続の可否、TTL値（16進数）をそれぞれ保持している。

【 0 0 4 4 】

この内、MACアドレス、PPPoEセッションID、及びIPアドレスは宛先となるユーザ端末を特定するために用いられる。グループIDは宛先ユーザ端末との認証に用いられる。キャリア網接続の可否はショートカット通信を行うか否かの判定に用いられる。TTL値については上記の通りである。

【 0 0 4 5 】

図3のフローチャートに戻って、イーサネット処理部32がフレーム24を受信した場合、制御部30が、TTL値に“1”を加算する（ステップS4）。

制御部30は、受信したフレームがキャリア網CN、すなわちエッジ装置18から送信されたフレーム25であるか否かを判定する（ステップS5）。

【 0 0 4 6 】

受信したフレームがエッジ装置18から送信されたフレーム25であると判定された場合は、イーサネット処理部32は、エッジ装置19,20との接続状態を確認する。この結果、エッジ装置19,20との接続を遮断している場合はフレーム25を処理する必要がないので、再度ステップS2に戻り、フレームの受信待ち状態となる（ステップS6）。

【 0 0 4 7 】

キャリア網CNとの接続を遮断しておらず、フレームを受信している状態では、イーサネット処理部32は、通常のスイッチング処理によりフレームを処理してステップS2に戻る（ステップS7）。

情報監視部33は、受信したフレーム24の内容を識別する（ステップS8）。情報監視部33による識別の結果、制御部30は、受信したフレーム24に送信元MACアドレス、PPPoEセッションID、及びIPアドレスが含まれているか否かを判定し、含まれていなければステップS10に、含まれていればステップS15に進む（ステップS9）。

【 0 0 4 8 】

情報監視部33は、フレーム24中に、後述する拡張PPPoEのデータが含まれているかどうかを判定する（ステップS10）。含まれていなければS7に進み、通常のスイッチング処理を行う。

フレーム24中に拡張PPPoEのデータが含まれている場合、情報監視部33は、フレームの種別を判定する（ステップS11）。ショートカット通信開始を示すフレームの場合はステップS12以降の認証処理に進み、違う場合はステップS23に進む。

【 0 0 4 9 】

図6にショートカット通信開始時のフレーム24のフォーマットを示す。

このショートカット通信開始時のフレーム24は通常の如く、物理層、データリンク層、ネットワーク層、トランスポート層、セッション層、プレゼンテーション層、アプリケーション層の7つの層により構成されている。

【 0 0 5 0 】

なお、ネットワーク層より上位層はネットワーク上の各領域において変更されることが無く共通であり、物理層はケーブルやコネクタ等に関するものに過ぎないため、以下のフレームの説明においては、図1について説明したように、本発明で内容の変更を伴うデータリンク層についてのみ説明する。

【 0 0 5 1 】

このデータリンク層を構成するMACアドレスとはネットワーク上の各端末に固有に定められたアドレスであり、フレーム中には宛先MACアドレスと発信元MACアドレスが書かれている。例えば、ONU13から通信装置15にフレームが送信される場合、宛先MACアドレスには通信装置15のMACアドレスが書かれ、発信元MACアドレスにはONU13のMACアドレスが書かれている。

【 0 0 5 2 】

そして他の端末にフレームを転送する場合は、通信装置15は、宛先MACアドレスを宛先の端末に合わせて書き換え、発信元MACアドレスを通信装置15のMACアドレスに書き換える。

次に書かれるPPPoEのプロトコルは、上位層識別子、バージョン、タイプ、コード、PPPoEセッションID、及びデータ長により構成される。これらの構成は、通常の通信におけるフレーム構成と同じである。

【 0 0 5 3 】

上記のPPPoEのプロトコルに続き、PPPoEの拡張部分（上記の拡張PPPoE）としてPPPoEのプロトコルにカプセル化される形で、ショートカット通信開始のTAGタイプ、TAGデータ長、グループIDのTAGタイプ、TAGデータ長、グループID、パスワードのTAGタイプ、TAGデータ長、及びパスワードが書かれる。

【 0 0 5 4 】

グループIDの決定方法としては、ショートカット通信を行うユーザ同士が、メールやチャット、あるいは電話等のコミュニケーション手段を用いて事前に決めておくことや、例えばオンラインゲームの事業者が、キャリア網から、該当ユーザがショートカット通信可能であるか否かの情報をリアルタイムに入手して、自動的にグループIDを割り当てることも可能である。

【 0 0 5 5 】

この拡張PPPoEに含まれる構成が従来のPPPoEの Protokol との相違点であり、ショートカット通信のTAGタイプの有無がショートカット通信開始か否かの判定に用いられる（ステップS11）。

このステップS11において、ユーザ端末11, 12からフレーム24がショートカット通信の開始を要求していることが分かったとき、両者のグループIDが一致することでユーザ端末11, 12間のショートカット通信を許可したと仮定すると、何らかの手段により、悪意を持った第三者がグループIDを入手することにより、ショートカットグループ間通信に侵入する可能性がある。

【 0 0 5 6 】

この悪意の侵入を防ぐ手段として、ここではパスワードを用いてRADIUSサーバ21（図1参照）と連携するユーザ認証を用いる。もちろん、グループIDのみでショートカット通信を許可してもよいし、RADIUSサーバ21と連携せずに、制御部30がユーザ認証を行ってもよい。

【 0 0 5 7 】

RADIUS制御部34は、図7に示すフレームを生成し、RADIUSサーバ21に送信する（ステップS12）。このフレームは現在RFC2865で定義され、使用されているRADIUSのフレームフォーマットそのものである。

その後の動作は認証方式によって、若干異なるが最終的にはRADIUSサーバから通信装置に対して認証OKかNGの回答フレームが返信される。このシーケンスに関しても、RFC2865で規定されているものをそのまま使用する。

【 0 0 5 8 】

なお、この場合の構成は、データリンク層に宛先MACアドレス及び発信元MACアドレスが書かれ、ネットワーク層（IP）に上位層識別子、バージョン、タイプ、サービスタイプ（TOS）、データ長、識別子、フラグ、フラグメントオフセット、TTL、上位層識別子（UDP）、ヘッダチェックサム、発信元IPアドレス、及びRADIUSサーバのIPアドレスが書かれる。

【 0 0 5 9 】

トランスポート層に発信元ポート番号、宛先ポート番号、データ長、UDPチェックサムが書かれ、その上位層にコード（アクセスリクエスト）、識別子、デー

タ長、認証リクエスト、グループID（タイプ及びデータ長を含む）、パスワード（タイプ及びデータ長を含む）、通信装置のIPアドレス（タイプ及びデータ長を含む）、タイプ（NASポート）、データ長、及び通信装置のポートが書かれる。

【 0 0 6 0 】

次にRADIUS制御部34は、認証が成功したか否かを判定する（ステップS13）。認証が成功しなかった場合はショートカット通信ができないので、ステップS2に戻ってフレーム待ちとなる。

認証に成功した場合、制御部30は、メモリ31上に展開された図5に示すテーブルTBLに受信したグループIDを書き込む（ステップS14）。全く同様の手順でユーザ端末12からショートカット通信の開始要求を受け、認証を行った後、グループIDが書き込まれる。

【 0 0 6 1 】

ステップS9に戻って、受信したフレームに送信元MACアドレス、PPPoEセッションID、及びIPアドレスが含まれている場合について説明する。

受信したフレーム24に、送信元MACアドレス、PPPoEセッションID、及びIPアドレスが含まれている場合、情報監視部33は、メモリ31上のテーブルTBLを参照してフレーム24に書かれている送信元IPアドレスと同じIPアドレスに対応したポートがあるか否かを判定する（ステップS15）。

【 0 0 6 2 】

同じIPアドレスがない場合、テーブルTBL上にユーザ端末11の情報が無いことを意味するので、制御部30は、テーブルTBLにユーザ端末11に対応するMACアドレス、PPPoEセッションID、及びIPアドレス等の情報を新規に書き込む（ステップS16）。

【 0 0 6 3 】

ステップS15で、同じIPアドレスがある場合、制御部30は、さらにそのIPアドレスのポートのMACアドレス及びPPPoEセッションIDと、フレーム24のMACアドレス及びPPPoEセッションIDとを比較して同じであるか否かを判定する（ステップS17）。

【 0 0 6 4 】

両者が一致しない場合、制御部30は、フレーム24の内容に合わせてテーブルTBLの内容を変更する（ステップS18）。

ステップS17において、ポートの情報とフレーム24の情報が一致した場合、情報監視部33は、フレーム24に書き込まれたグループIDを確認する。グループIDが“0”の場合はグループIDが設定されていないから、ショートカット通信を行うことはできず、ステップS7に戻り、通常のスイッチング処理によりフレーム24を処理する（ステップS19）。

【0065】

グループIDが“0”でない場合、制御部30は、テーブルTBLに記憶されているポートP1,P2の情報を比較し、同一のグループIDで且つ宛先IPアドレスと同じIPアドレスを持つユーザ端末があるか否かを判定する（ステップS20）。なお、宛先ユーザ端末のグループIDは、予め図5に示すテーブルTBLに用意する他、該宛先ユーザ端末から受信してもよい。

【0066】

グループID及びIPアドレスが一致すると判定された場合、制御部30は、受信したフレーム24を折り返してユーザ端末12に送信するため、フレーム24のデータリンク層に書かれている宛先MACアドレス、送信元MACアドレス、及びPPPoEのセッションIDの情報をユーザ端末12に該当する情報に書換える。そして制御部30は、図6に示すフレーム24をユーザ端末12に向けて送信する（ステップS21）。

【0067】

図8にショートカット通信中のフレームフォーマットを示す。

宛先MACアドレス、発信元MACアドレス、及びPPPoEのプロトコルの構成については図6のショートカット通信開始の場合と同様であるので説明は省略する。

また、同様にPPPoEのプロトコルの拡張部分が続くが、この構成はショートカット通信開始の場合と異なる。すなわち、このPPPoE拡張部分には、上位層識別子、バージョン、タイプ、TOS、データ長、識別子、フラグ、フラグメントオフセット、TTL、上位層識別子、ヘッダチェックサム、発信元IPアドレス、及び宛先IPアドレスが書かれる。これらの構成は、通常の通信においてフレームのネットワーク層に書かれる構成と同じである。つまりネットワーク層に書かれる構成

と同じものがPPPoE拡張部分にも書かれることになる。

【 0 0 6 8 】

なぜなら、IPアドレスは、図5に示すテーブルTBLを用いてショートカット通信の可否を判定するのに必要であるが、通信装置15は、物理層及びデータリンク層の情報しか読むことができないので、通信装置15がデータリンク層の情報を読む如くでIPアドレスを読むことができるようにするためである。

【 0 0 6 9 】

ステップS16において、グループID及びIPアドレスが一致しないと判定された場合、制御部30は、キャリア網CNとの接続の状態を確認する。キャリア網CNとの接続を遮断している状態ではフレームを処理する必要がないので、再度ステップS2に戻り、フレームの受信待ち状態へと進む。

【 0 0 7 0 】

キャリア網CNとの接続を遮断しておらず、受信している状態の場合はステップS7に戻り、通常のスイッチング処理によりフレーム24を処理する（ステップS22）。

ステップS11に戻り、フレーム24がショートカット通信開始を示すデータを含まない場合について説明する。

【 0 0 7 1 】

情報監視部33は、フレーム24がショートカット通信を行っている同一グループ内から送信されたものか否かを判定する。同一グループ外からのフレームであればショートカット通信の当事者外からのフレームであるので、処理することなくステップS2に戻り、フレーム待ちの状態となる（ステップS23）。

【 0 0 7 2 】

受信したフレーム24が、図9に示すショートカット通信終了のフレームの場合、制御部30は、ショートカット通信を終了するよう、図5に示すテーブルTBL上のグループIDを“0”とする（ステップS24）。そして制御部30は、キャリア網CNとの接続を再開すべく、キャリア網接続可否のパラメータを0x0000とし（ステップS25）、ステップS2に戻ってフレーム待ちとする。

【 0 0 7 3 】

図9にショートカット通信終了のフレームフォーマットを示す。

宛先MACアドレス、発信元MACアドレス、及びPPPoEのプロトコルの構成については図6のショートカット通信開始の場合と同様であるので説明は省略する。

次に、同様にPPPoEのプロトコルの拡張部分については、ショートカット通信開始の場合と同様である。ただし、TAGタイプの種類がショートカット通信開始ではなくショートカット通信終了を示す内容となっている。このTAGタイプが、ショートカット通信終了の可否を判定するのに用いられる。

【 0 0 7 4 】

受信したフレーム24が、図10に示すショートカット通信中断のフレームの場合、制御部30は、キャリア網CNとの接続を一時中断すべく、キャリア網接続可否のパラメータを0x0001とし（ステップS26）、ステップS2に戻ってフレーム待ちとなる。

【 0 0 7 5 】

図10にキャリア接続中断のフレームフォーマットを示す。PPPoEのプロトコル及び拡張部分ともショートカット通信終了の場合と同じであるので説明を省略する。

同様に、TAGタイプの種類はショートカット通信開始ではなくキャリア接続中断を示す内容となっている。このTAGタイプが、キャリア接続中断の可否を判定するのに用いられる。

【 0 0 7 6 】

受信したフレーム24が、図11に示すショートカット通信再開のフレームの場合、制御部30は、キャリア網CNとの接続を再開すべくステップS25に進む。

図11にキャリア接続再開のフレームフォーマットを示す。PPPoEのプロトコル及び拡張部分ともショートカット通信終了の場合と同じであるので説明を省略する。

【 0 0 7 7 】

同様に、TAGタイプの種類はショートカット通信開始ではなくキャリア接続再開を示す内容となっている。このTAGタイプが、キャリア接続再開の可否を判定するのに用いられる。

次に、ユーザ端末11、12の処理について説明する。

【0078】

図12はユーザ端末11、12の構成の実施例を示しており、この実施例では、制御部41、アプリケーション42、メモリ43、イーサネット処理部44、PPPoE処理部45により構成されている。これらの内部は、CPU、ROM、RAM等を用いることにより構成される（図示せず）。

【0079】

制御部41は、フレームの作成等ユーザ端末11の全体的な制御を行う。メモリ31は、制御部41の動作に必要な情報を保持する。イーサネット処理部44は、イーサネットのプロトコルによる通信処理を行う。PPPoE処理部45は、PPPoEプロトコルやその拡張形式であるTAG タイプ等をフレーム中に作成する。

【0080】

図13は本発明におけるユーザ端末の動作実施例（1）のフローチャート図を示したものである。図4に示したTTL値の処理についての説明、図5に示すテーブルTBLの内容の説明、及び図6～11に示すフレームの内容は、通信装置15の説明と共通するので必要に応じて参照する。以上の各図を用いて、実施例（1）におけるユーザ端末側の動作を説明する。

【0081】

電源投入後、ユーザ端末11でインターネットへのアクセスが指示されると、PPPoE処理部45は、ONU13及び通信装置15を介してエッジ装置18と接続するための処理を開始する（ステップS31）。ユーザ端末11は、通常のPPPoEの処理に従ってインターネット接続を行う（ステップS32）。

【0082】

次に、制御部41は、ユーザAからアプリケーション42を介して入力があったか否か判定し、入力がなければステップS32に戻り、通常の通信処理を行う（ステップS33）。

ユーザAから入力があった場合、制御部41は、入力がショートカット通信開始の指示であるか否かを判定し（ステップS34）、入力がショートカット通信開始の指示であれば、制御部41は、その指示の中でグループIDが設定されているか否

かを判定する（ステップS35）。

【 0 0 8 3 】

グループIDが設定されていれば、ユーザ端末11の制御部41は、ユーザBと一緒に決めたグループID、パスワード、及びユーザ端末Bに割り当てられているIPアドレスをユーザ端末11の通信ソフトに設定し、ショートカット通信の機能をONにする。

【 0 0 8 4 】

そして、ユーザ端末11のPPPoE処理部44及びイーサネット処理部45は、図7に示すフレーム23を作成して送出する（ステップS36）。

グループIDが設定されていなければ、制御部41は、アプリケーション42を介してエラー表示をし、ステップS33のユーザ入力に戻る（ステップS37）。

【 0 0 8 5 】

ステップS34でユーザ入力ショートカット通信開始でなかった場合、制御部41は、入力がショートカット通信終了の指示であるか否かを判定する（ステップS38）。

ショートカット通信終了の場合は、図1及び図9に示したフレーム23を作成して送出する（ステップS39）。

【 0 0 8 6 】

ステップS38で、ショートカット通信終了でなかった場合は、制御部41は、入力がショートカット通信中断の指示であるか否かを判定する（ステップS40）。

ショートカット通信中断の場合は、図10に示したフレーム23を作成して送出する（ステップS41）。

【 0 0 8 7 】

ステップS40で、ショートカット通信中断でなかった場合は、制御部41は、入力がショートカット通信再開の指示であるか否かを判定する（ステップS42）。

ショートカット通信再開の場合は、図11に示すフレーム23を作成して送出する（ステップS43）。

【 0 0 8 8 】

実施例（2）：図14～16

次に、ショートカット通信中のフレーム24をPPPoEプロトコルの拡張ではなく、イーサネット上でカプセル化する場合の図2に示した通信装置15の動作実施例(2)について説明する。

【 0 0 8 9 】

図14は、この動作実施例(2)における通信装置のフローチャートを示したものであり、図15は、動作実施例(2)におけるショートカット通信中のユーザ端末11と通信装置15との間でやり取りされるフレームのフォーマットを示したものである。

【 0 0 9 0 】

以下、これらの図を用いて通信装置の実施例(2)について説明する。なお、動作実施例(1)と共通する動作については実施例(1)と同じ符号を用いてその説明は省略する。

まず、実施例(1)のステップS1～S8にそれぞれ対応したステップS51～S58を実行する。

【 0 0 9 1 】

次に情報監視部33は、受信したフレームに送信元MACアドレス、PPPoEセッションID、及びIPアドレスが含まれているか否かを判定し、含まれていなければステップS53に戻る(ステップS59)。

受信したフレーム24に送信元MACアドレス、PPPoEセッションID、及びIPアドレスが含まれている場合、情報監視部33は、受信したフレーム24にイーサネット上に直接カプセル化した送信元IPアドレスがあるか否かを判定する(ステップS60)。

【 0 0 9 2 】

受信したフレーム24にイーサネット上に直接カプセル化した送信元IPアドレス等がない場合、実施例(1)のステップS10～S14にそれぞれ対応したステップS61～S65を実行する。ここで、図6及び図7に示すフレーム24を用いた、RADIUSによる認証を含むショートカット通信の開始処理が行なわれる。

【 0 0 9 3 】

なお、ショートカット通信の開始処理は拡張PPPoEにより行なった実施例(1)

と同様である。

受信したフレーム24にイーサネット上に直接カプセル化した送信元IPアドレス等がある場合、実施例（1）のステップS15～S22にそれぞれ対応したステップS66～S73を実行することで、フレーム24を送信すべきか否かの判定及びフレームの送信処理を行なう。

【 0 0 9 4 】

図15にイーサネットに直接カプセル化した場合のフレーム24を示す。これは、図8に示した拡張PPPoEによる場合と異なり、PPPoEのプロトコルが除かれており、PPPoEの拡張部分に相当する、発信元IPアドレス、宛先IPアドレス等がイーサネットに直接カプセル化された形で書かれている。

【 0 0 9 5 】

また、ステップS11に対応したステップS62においてショートカット通信開始でないと判定された場合、実施例（1）のステップS23～S26にそれぞれ対応したステップS74～S77を実行する。ここで、図9、図10、及び図11に示すフレーム24を用いた、ショートカット通信の終了・中断・再開処理が行なわれる。

【 0 0 9 6 】

なお、ショートカット通信の開始・終了・中断・再開処理はいずれも拡張PPPoEにより行なうため実施例（1）と同じ動作になる。

次に、ユーザ端末11における動作実施例（2）について説明する。この場合の構成は図12に示したものをを用いる。

【 0 0 9 7 】

図16は、この動作実施例（2）のフローチャートを示したものであり、実施例（1）と共通する図については随時参照しながら説明する。

まずステップS31に対応するステップS81を実行する。次に制御部41は、“1”のときにショートカット通信中を示すフラグSCが1か否かを判定する（ステップS82）。

【 0 0 9 8 】

フラグSCが“1”の場合、制御部41は、“1”のときにショートカット通信が中断中であることを示すフラグCSが“1”か否かを判定する（ステップS83）。

フラグCSが“1”のときは、イーサネット処理部44は、ショートカット先へはフレーム23をイーサネット上にカプセル化して送信し、ショートカット先以外へは送信しないよう処理する（ステップS84）。

【0099】

フラグCSが“0”のときは、ショートカット先へは、イーサネット処理部44は、フレーム23をイーサネット上にカプセル化して送信する。一方、ショートカット先以外へは、PPPoE処理部45は、フレーム23をPPPoE上にカプセル化して送信する（ステップS85）。なお、ステップS84又はステップS85が終わったらステップS87へ進む。

【0100】

次に、ステップS32～37にそれぞれ対応するステップS86～90を実行する。なおステップS90では、ショートカット通信開始となるので、フレーム23の送信と共にフラグSCを“1”とする。

ステップS88でショートカット通信開始のフレーム23で無いことが分かった場合は、ステップS38～39に対応するステップS92～93を実行する。なおステップS93では、ショートカット通信終了となるので、フレームの送信と共に制御部41は、フラグSCを“0”とする。

【0101】

ステップS92で、ショートカット通信終了でなかった場合は、制御部41は、入力がショートカット通信中断の指示であるか否かを判定する（ステップS94）。

ショートカット通信中断の場合は、フラグCSを“1”にし（ステップS95）、イーサネット処理部44は、図10に示すフレーム23を作成して送出する（ステップS96）。

【0102】

ステップS40で、ショートカット通信中断でなかった場合は、制御部41は、入力がショートカット通信再開の指示であるか否かを判定する（ステップS97）。

ショートカット通信再開の場合は、制御部41は、フラグCSを“1”にし（ステップS98）、イーサネット処理部44は、図11に示すフレーム23を作成して送出する（ステップS99）。

【 0 1 0 3 】

(付記 1)

ユーザ端末とネットワーク接続業者機器との間の通信を行う接続処理部と、
送信元のユーザ端末から送信されたデータに含まれるデータリンク層情報を読み出し、該データリンク層情報にネットワーク接続業者機器への通信要求情報又は宛先ユーザ端末とのショートカット通信の要求情報が含まれているか否かを監視する情報監視部と、

該データリンク層情報が該通信要求情報を含む場合には該ネットワーク接続業者機器に該データを出力し、該データリンク層情報が該ショートカット通信の要求情報を含む場合には該宛先ユーザ端末に該データを出力する制御部と、

を備えることを特徴とした通信装置。

【 0 1 0 4 】

(付記 2) 付記 1 において、

該ショートカット通信の要求情報は、該データリンク層情報にカプセル化されていることを特徴とする通信装置。

(付記 3) 付記 2 において、

該ショートカット通信の要求情報は、該データリンク層情報中のイーサネットのプロトコルにカプセル化されていることを特徴とする通信装置。

【 0 1 0 5 】

(付記 4) 付記 2 において、

該通信要求情報は PPPoE のプロトコルであり、該ショートカット通信の要求情報は、該データリンク層情報中の該 PPPoE のプロトコルにカプセル化されていることを特徴とする通信装置。

【 0 1 0 6 】

(付記 5) 付記 1 から 4 のいずれかにおいて、

該データリンク層情報は認証情報を含み、該制御部は、該認証情報に基づいて該送信元ユーザ端末と該宛先ユーザ端末とのショートカット通信を許容するか否かを判定し、該ショートカット通信を許容する場合に、該接続処理部に該宛先ユーザ端末へ該データを出力させることを特徴とする通信装置。

【 0 1 0 7 】

(付記 6) 付記 5 において、

該認証情報はRADIUSのフォーマットに基づく形式で記述されており、該制御部は該認証情報をRADIUSサーバに出力してその照合結果を参照することでショートカット通信を許容するか否かを判定することを特徴とする通信装置。

【 0 1 0 8 】

(付記 7) 付記 1 から 6 のいずれかにおいて、

該制御部は、該送信元ユーザ端末及び該宛先ユーザ端末のアドレス情報を通信ポートに対応付けて保持するメモリを備え、該データが該ショートカット通信の要求情報を含む場合に、該ショートカット通信の要求情報に含まれるアドレス情報に対応した通信ポートを通して該接続処理部に該データを出力させることを特徴とする通信装置。

【 0 1 0 9 】

(付記 8) 付記 1 から 7 のいずれかにおいて、

該情報監視部が該通信要求情報を読み出した結果、該ネットワーク接続業者機器との接続の中断要求情報が含まれている場合、該接続処理部は該ネットワーク接続業者機器との通信を中断することを特徴とする通信装置。

【 0 1 1 0 】

(付記 9) 付記 1 から 8 のいずれかにおいて、

該制御部は、該データリンク層情報に含まれるMACアドレスの書き換えにより該データの出力先を制御することを特徴とする通信装置。

(付記 1 0) 付記 1 から 9 のいずれかにおいて、

該制御部は、該送信元ユーザ端末からの該データリンク層情報に含まれる認証情報と該宛先ユーザ端末からの認証情報を照合することにより、該送信元ユーザ端末と該宛先ユーザ端末とのショートカット通信を許容するか否かを判定することを特徴とする通信装置。

【 0 1 1 1 】

(付記 1 1) 付記 8 において、

該情報監視部が該通信要求信号を読み出した結果、該ネットワーク接続業者機

器との接続の再開要求情報が含まれている場合、該接続処理部は該ネットワーク接続業者機器との通信を再開することを特徴とする通信装置。

【 0 1 1 2 】

【発明の効果】

以上説明したように、本発明に係る通信装置によれば、送信元のユーザ端末から送信されたデータに含まれるデータリンク層情報を読み出し、該データリンク層情報がネットワーク接続業者機器への通信要求情報を含む場合には該ネットワーク接続業者機器に該データ群を出力するという既存のプロトコルによる通信機能を維持しつつ、該データリンク層情報が宛先ユーザ端末とのショートカット通信の要求情報を含む場合には直接該宛先ユーザ端末に該データを出力することができる。

【 0 1 1 3 】

これにより、送信元のユーザ端末から宛先ユーザ端末に出力されるデータ量が膨大になった場合でも該ネットワーク接続業者機器を必要以上に拘束する必要がなくなり、以って通信の高速化を図ることができる。

【図面の簡単な説明】

【図1】

本発明に係る通信装置の一実施例が適用されるネットワークの構成例を示した概略図である。

【図2】

本発明に係る通信装置の構成の一実施例を示したブロック図である。

【図3】

本発明に係る通信装置で実行される動作実施例（1）の制御プログラムを示したフローチャート図である。

【図4】

本発明に係る通信装置で実行される各動作実施例に用いられるTTLカウンタの制御プログラムを示したフローチャート図である。

【図5】

本発明に係る通信装置の各動作実施例において各ポートに対応する情報を保持

するテーブルを示した図である。

【図6】

本発明に係る通信装置の各動作実施例においてショートカット通信開始のときに受信するフレームのフォーマットを示した図である。

【図7】

本発明に係る通信装置の各動作実施例においてショートカット通信の認証を依頼するときに受信するフレームのフォーマットを示した図である。

【図8】

本発明に係る通信装置の動作実施例（1）においてショートカット通信中に受信するフレームのフォーマットを示した図である。

【図9】

本発明に係る通信装置の各動作実施例においてショートカット通信を終了するときに受信するフレームのフォーマットを示した図である。

【図10】

本発明に係る通信装置の各動作実施例においてショートカット通信を中断するときに受信するフレームのフォーマットを示した図である。

【図11】

本発明に係る通信装置の各動作実施例においてショートカット通信を再開するときに受信するフレームのフォーマットを示した図である。

【図12】

本発明に係る通信装置に用いられるユーザ端末の一実施例を示したブロック図である。

【図13】

本発明に係る通信装置に用いられるユーザ端末で実行される動作実施例（1）の制御プログラムを示したフローチャート図である。

【図14】

本発明に係る通信装置で実行される動作実施例（2）の制御プログラムを示したフローチャート図である。

【図15】

本発明に係る通信装置の動作実施例（２）においてショートカット通信中に受信するフレームのフォーマットを示した図である。

【図16】

本発明に係る通信装置に用いられるユーザ端末で実行される動作実施例（２）の制御プログラムを示したフローチャート図である。

【符号の説明】

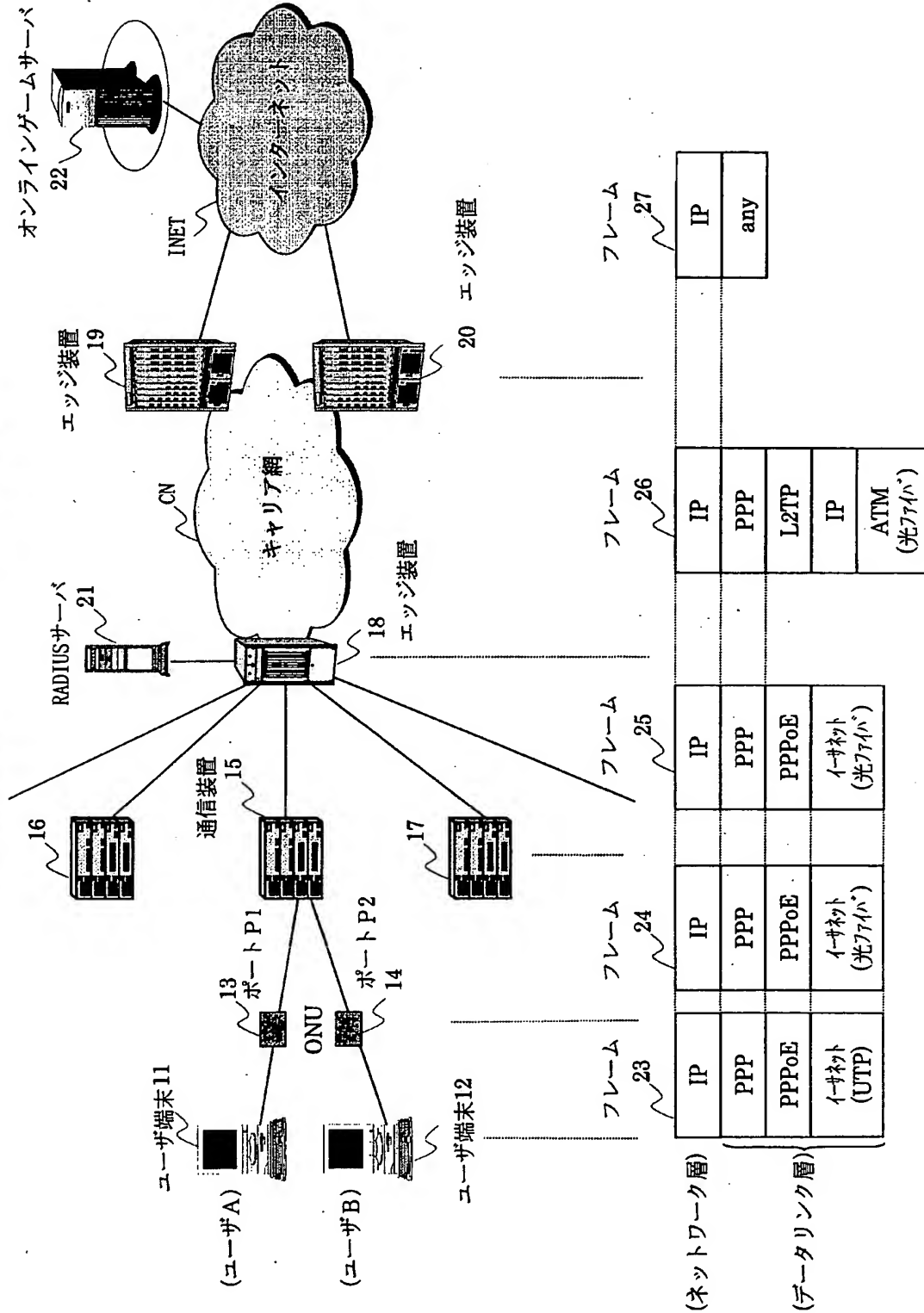
11, 12 ユーザ端末	13, 14 ONU
15, 16, 17 通信装置	18, 19, 20 エッジ装置
21 RADIUSサーバ	22 オンラインゲームサーバ
23 ユーザ端末からONUへのプロトコル	
24 ONUから通信装置へのプロトコル	
25 通信装置からエッジ装置へのプロトコル	
26 キャリア網におけるプロトコル	
27 インターネット上におけるプロトコル	
30 制御部	31 メモリ
32 イーサネット処理部	33 情報監視部
34 RADIUS制御部	41 制御部
42 アプリケーション	43 メモリ
44 イーサネット処理部	45 PPPoE処理部

図中、同一符号は同一又は相当部分を示す。

【書類名】 図面

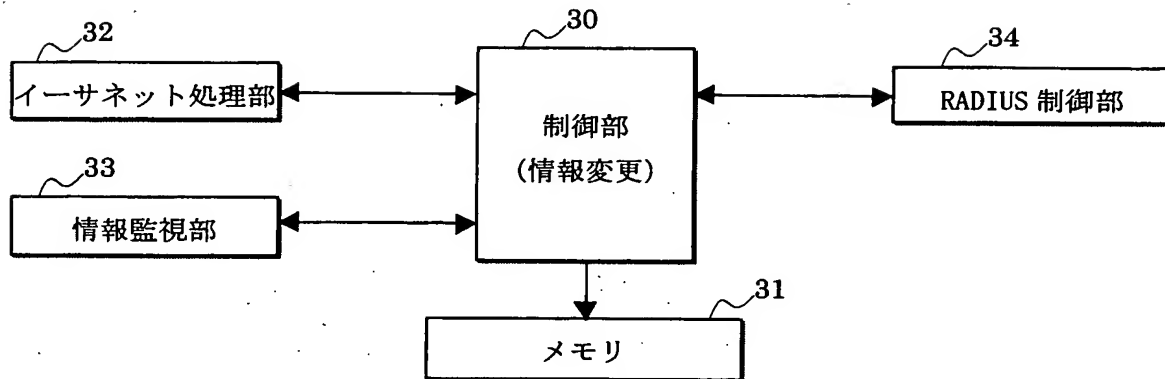
【図 1】

本発明が適用されるネットワークの構成例

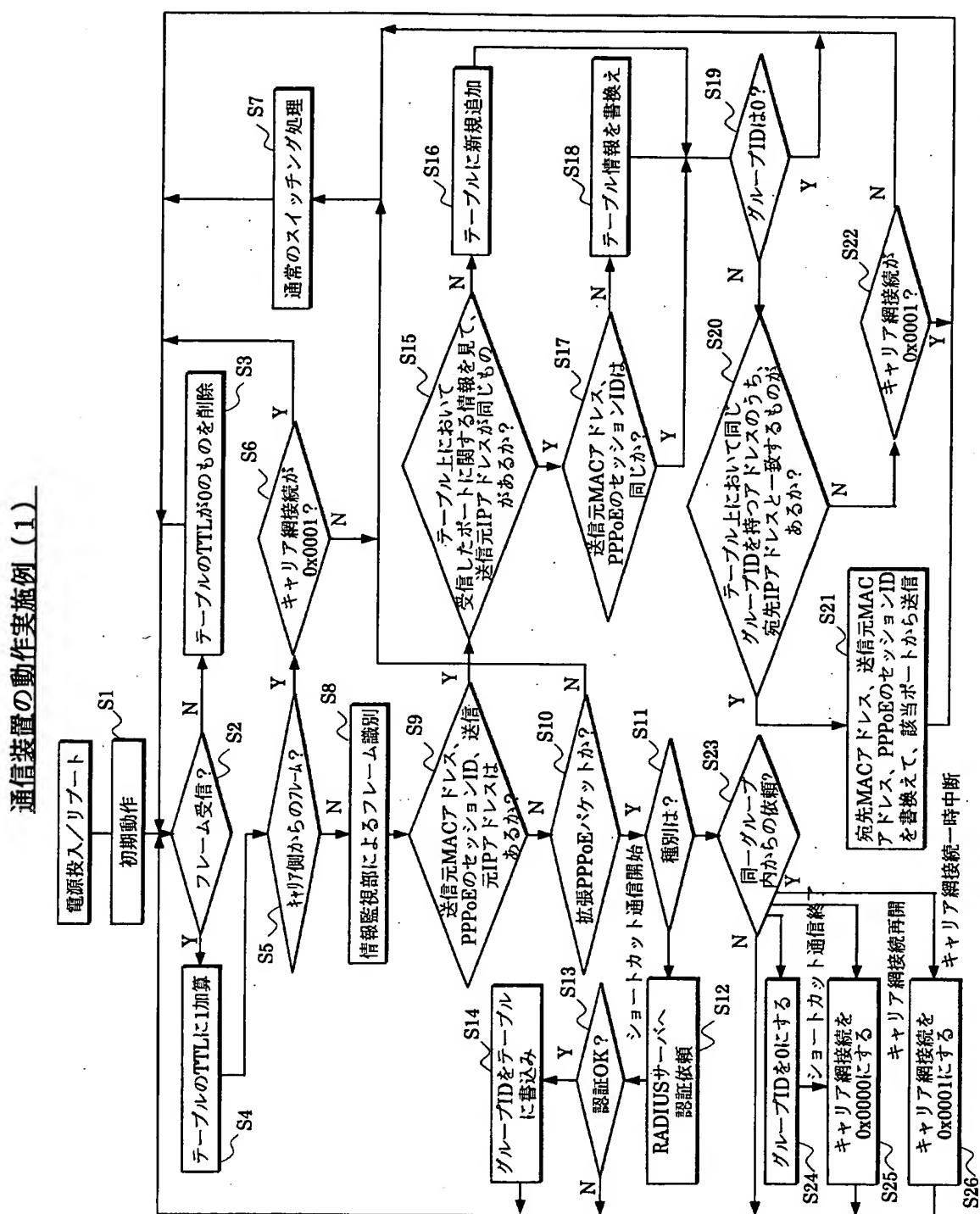


【図 2】

通信装置の構成例

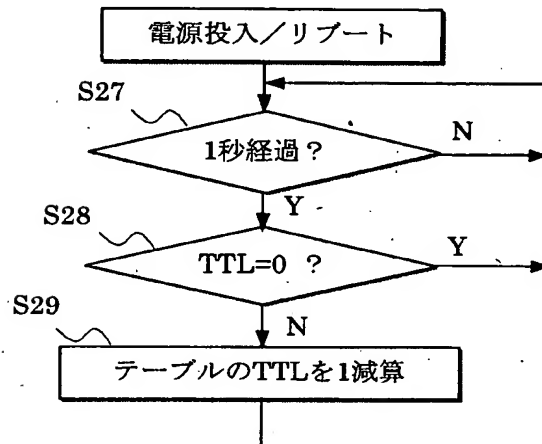


【図 3】



【図 4】

TTLのカウンタのフロー図



【図 5】

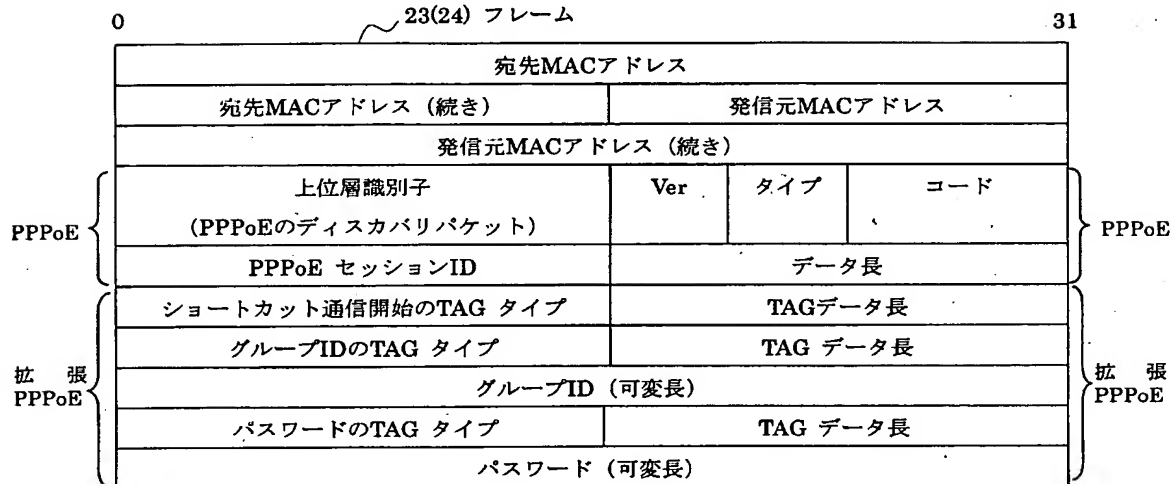
通信装置のポート情報保持テーブル例

TBL

ポート	MAC アドレス	PPPoE セッション ID	IP アドレス	グループ ID	キャリア網 接続の可否	TTL
P1	00:00:0E:11:22:xx	0x0001	112.116.5.xxx	0xFD376458	0x0001	0x0020
P2	00:00:0E:22:33:xx	0x0003	168.34.22.xxx	0xFD376458	0x0001	0x003E

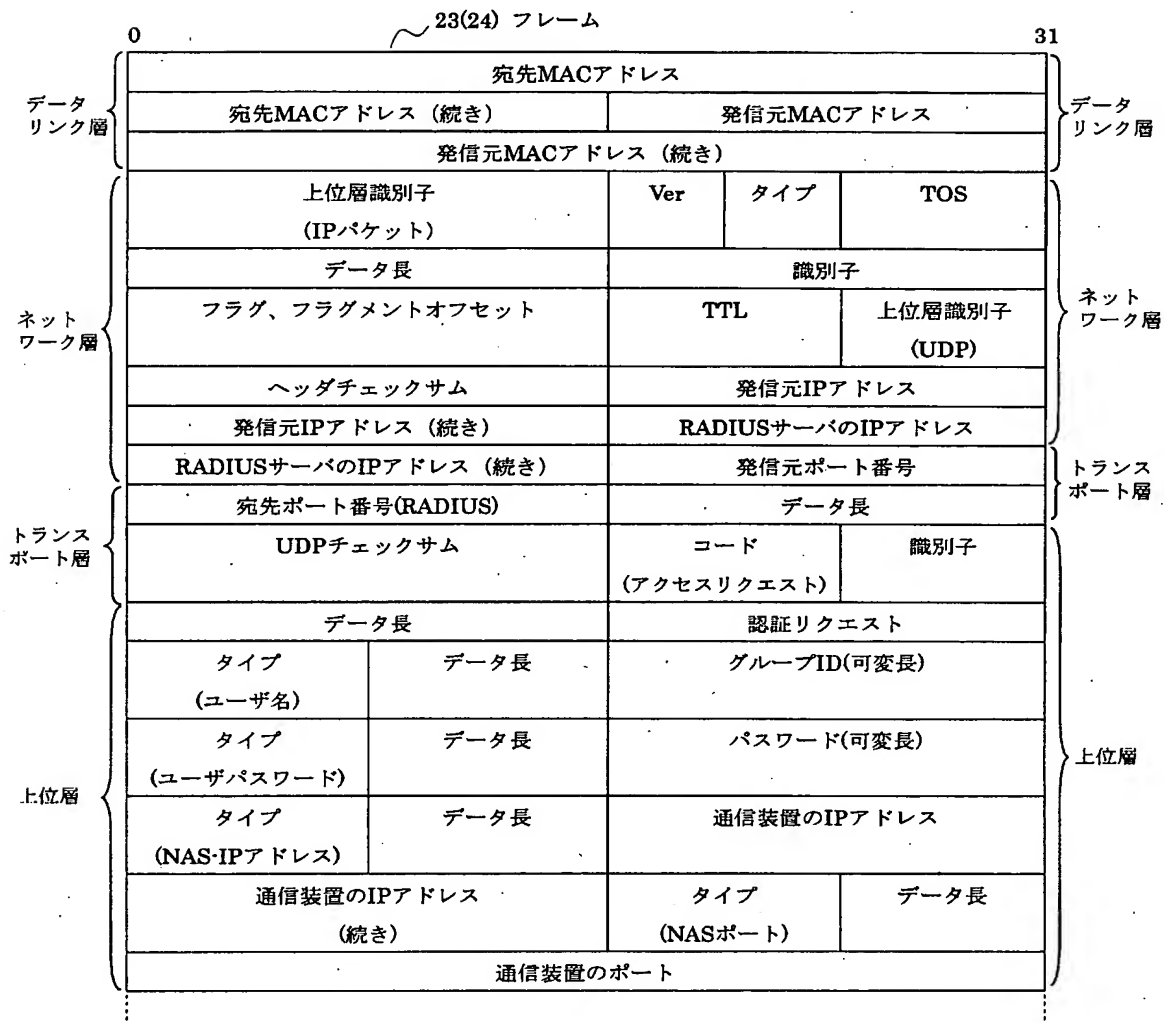
【図 6】

ショートカット通信開始フレームフォーマット



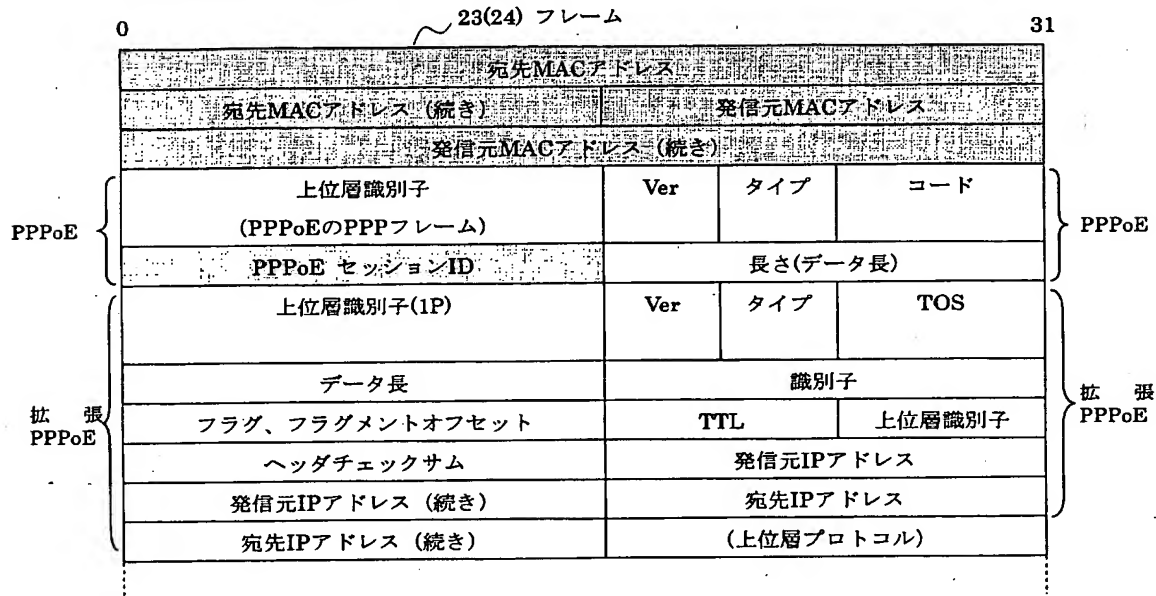
【図 7】

認証依頼フレームフォーマット



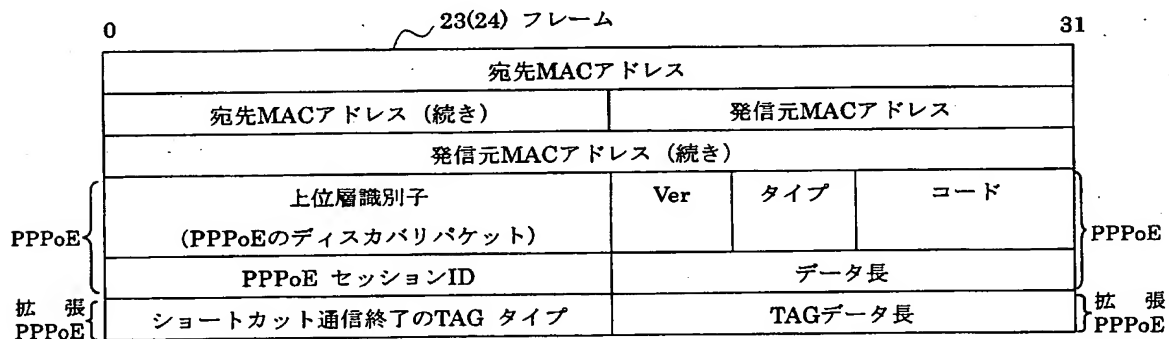
【図 8】

実施例 (1) におけるショートカット通信中のフレームフォーマット



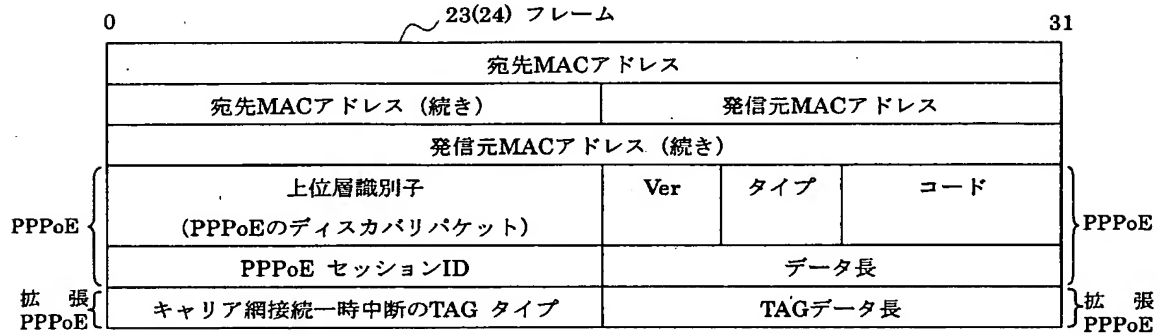
【図 9】

ショートカット通信終了フレームフォーマット



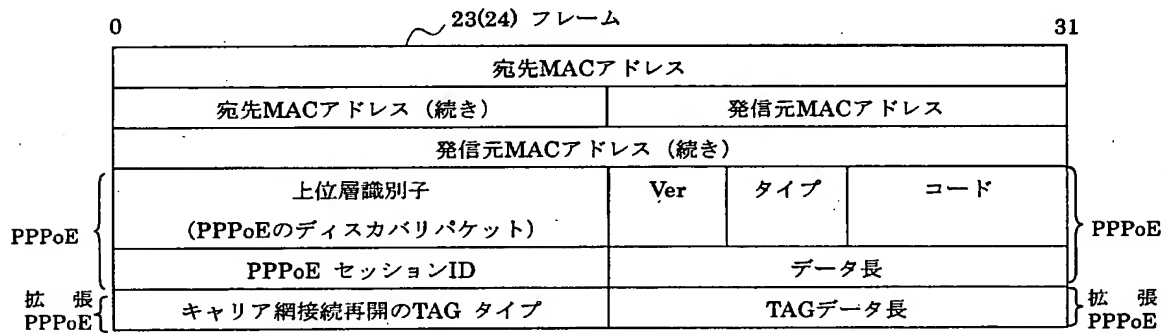
【図 1 0】

ショートカット通信一時中断フレームフォーマット



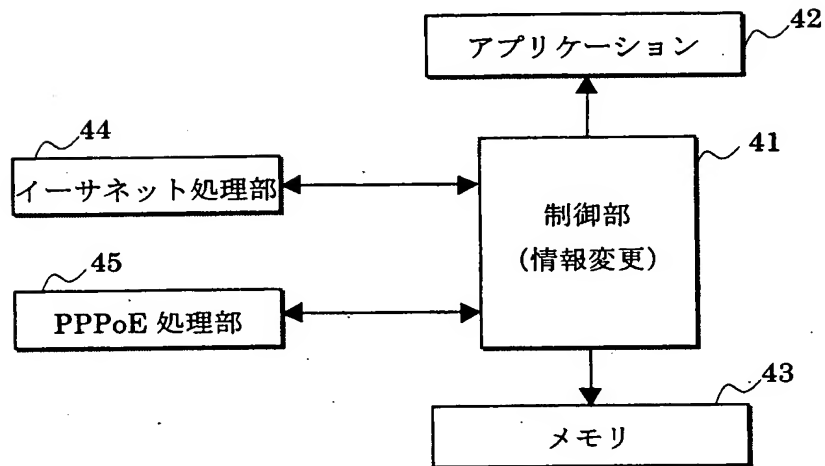
【図 1 1】

ショートカット通信再開フレームフォーマット



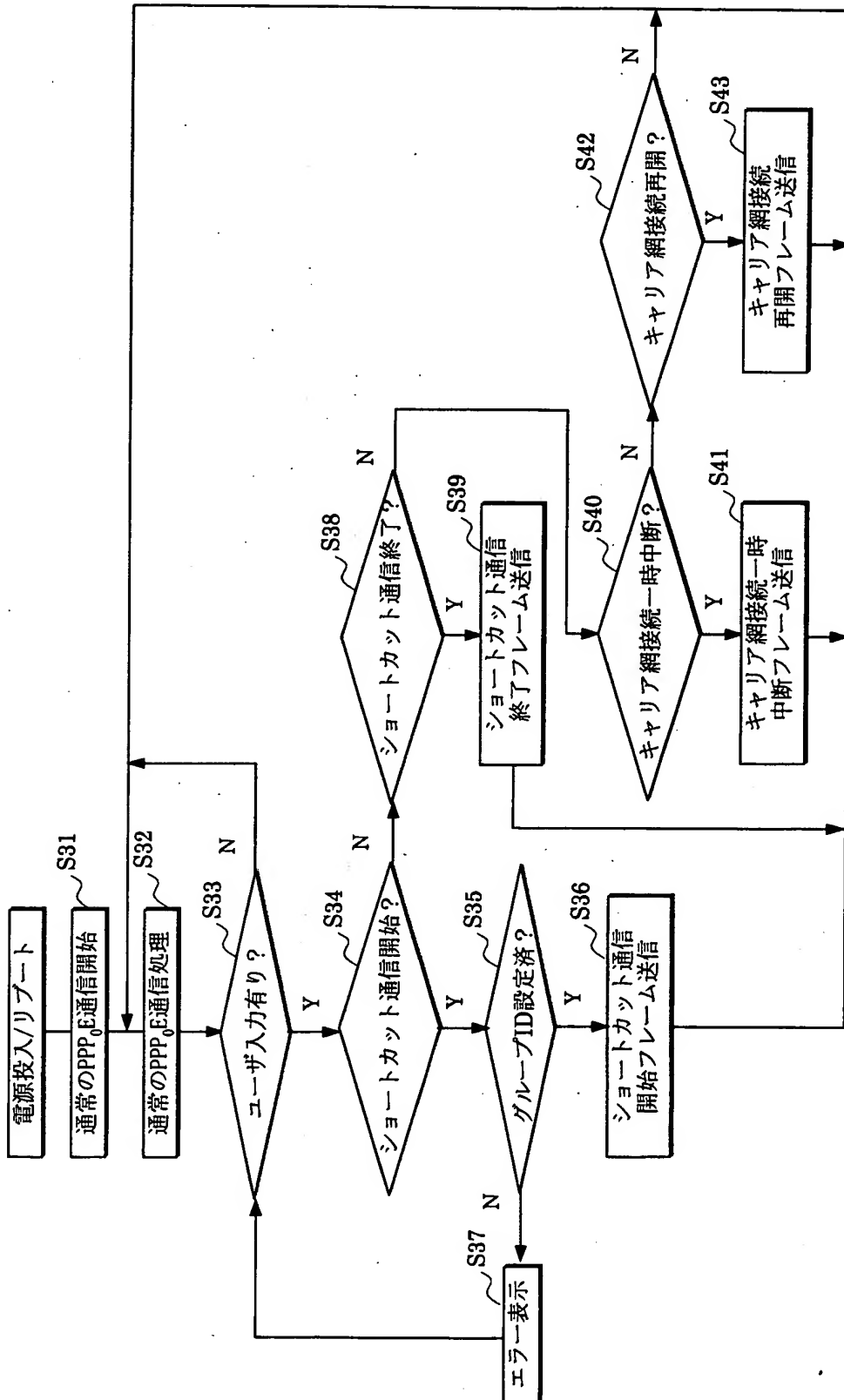
【図12】

ユーザ端末の構成例



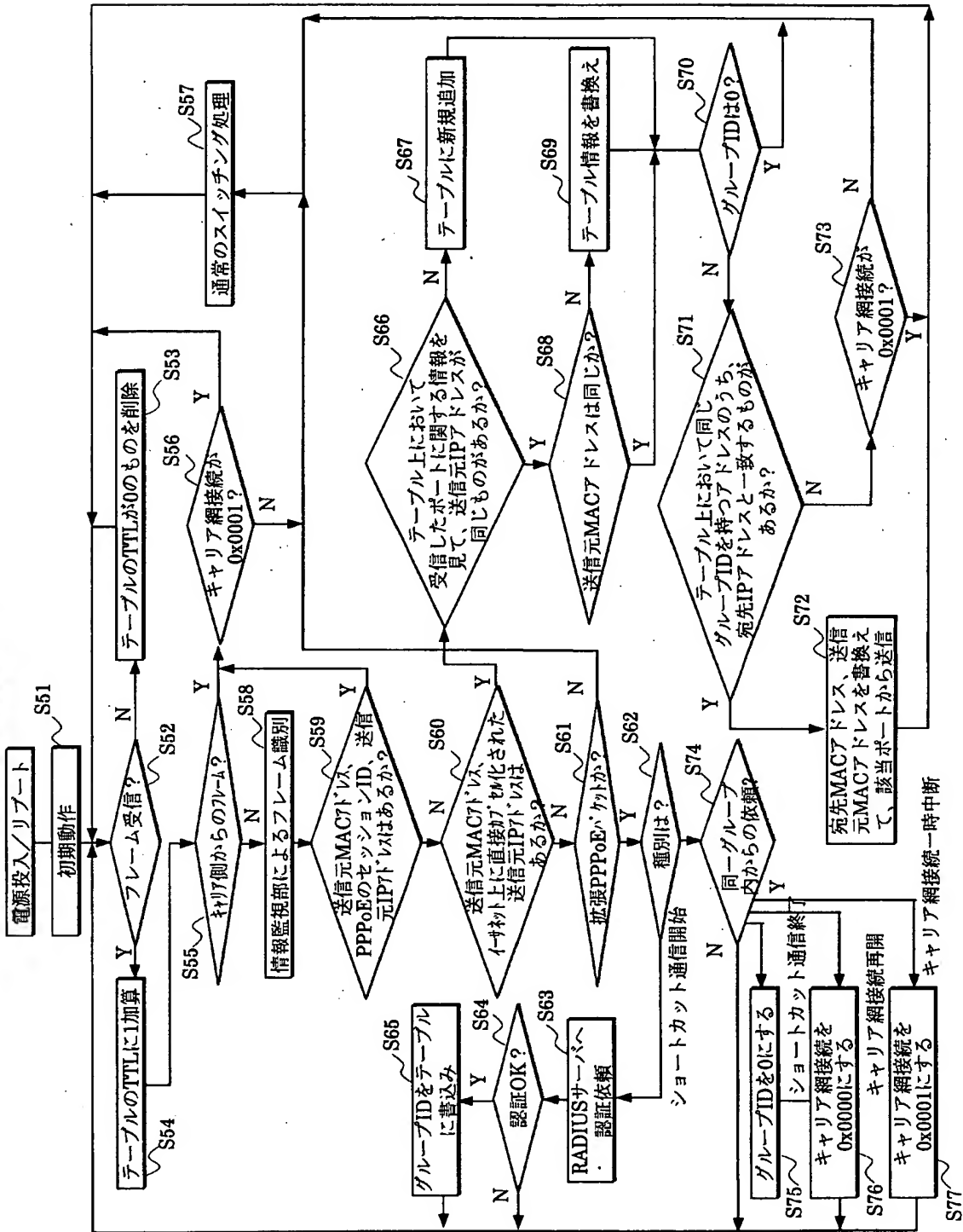
【図 13】

ユーザ端末の動作実施例 (1)



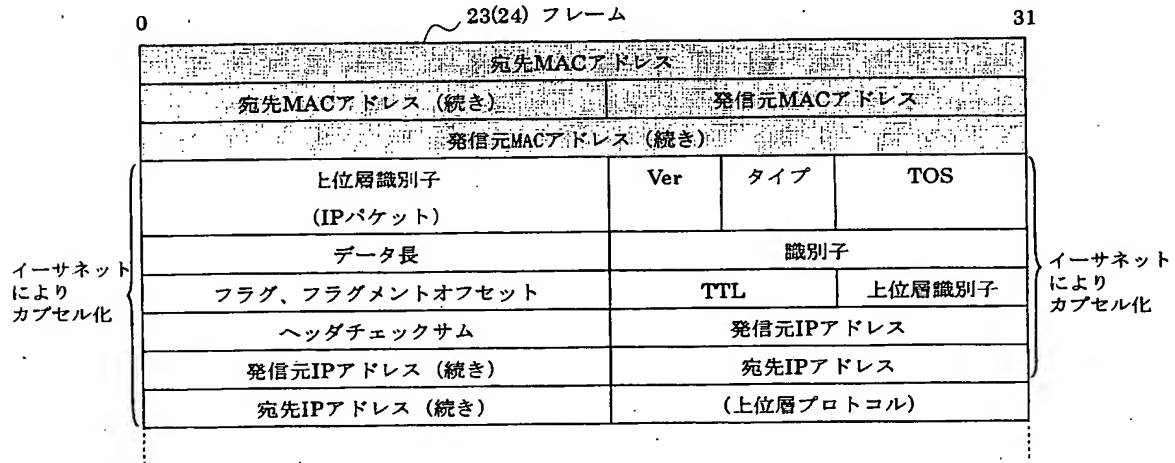
【図14】

通信装置の動作実施例 (2)



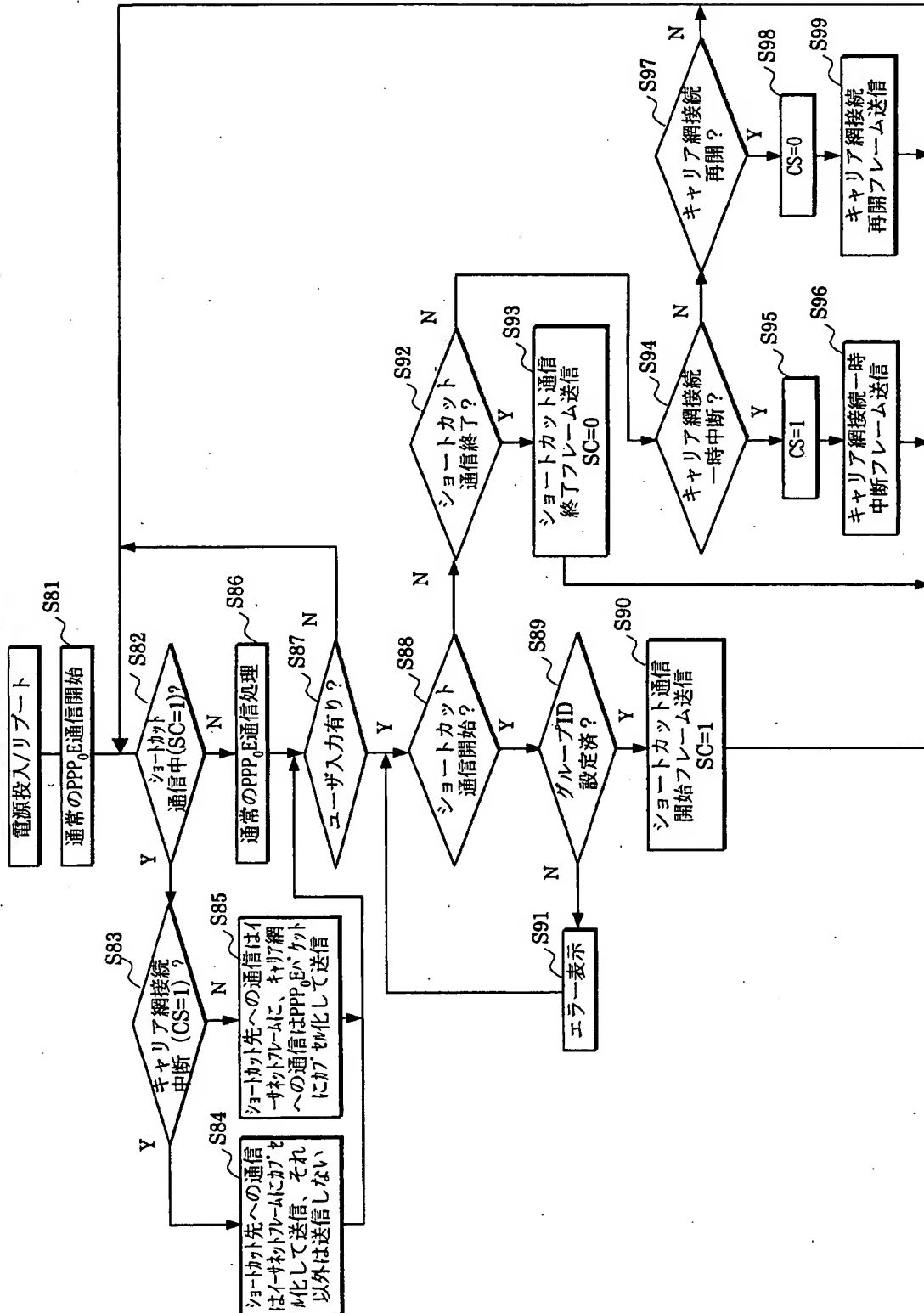
【図 1 5】

実施例（2）におけるショートカット通信中のフレームフォーマット



【図16】

ユーザ端末の動作実施例 (2)



【書類名】 要約書

【要約】

【課題】 ユーザ端末とネットワーク接続業者機器との間の通信を行う通信装置において、ユーザ端末間でショートカット通信させることにより通信の高速化を図る。

【解決手段】 送信元のユーザ端末11から送信されたデータ23に含まれるデータリンク層情報を読み出し、該データリンク層情報がネットワーク接続業者機器18への通信要求情報を含む場合には該ネットワーク接続業者機器18に該データ群を出力するという既存のプロトコルによる通信機能を維持しつつ、該データリンク層情報が宛先ユーザ端末とのショートカット通信の要求情報を含む場合には直接該宛先ユーザ端末に該データを出力する。

【選択図】 図8

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社